DIE UNLÖSBARKEIT DES ZEHNTEN HILBERTSCHEN PROBLEMS

Autor(en): **Hermes, Hans**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **18 (1972)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **27.04.2024**

Persistenter Link: https://doi.org/10.5169/seals-45360

DIE UNLÖSBARKEIT DES ZEHNTEN HILBERTSCHEN PROBLEMS

von Hans HERMES [1])

In diesem Jahr ist gezeigt worden, daß das zehnte Hilbertsche Problem unlösbar ist. Nachfolgend soll ein Bericht gegeben werden über die wesentlichen Schritte, die zu dem genannten Resultat geführt haben.

1. *Das zehnte Hilbertsche Problem.* Dieses Problem ist eines der 23 Probleme, die Hilbert anlässlich des internationalen Pariser Mathematikerkongresses im Jahre 1900 vorgelegt hat. Vor der Aufzählung seiner Probleme bemerkt Hilbert [3] [2]) u.a.:

„Mitunter kommt es vor, daß wir die Beantwortung (eines mathematischen Problems) unter ungenügenden Voraussetzungen erstreben und infolgedessen nicht zum Ziel gelangen. Es entsteht dann die Aufgabe, die Unmöglichkeit der Lösung des Problems... nachzuweisen. ... In der neueren Mathematik spielt die Frage nach der Unmöglichkeit gewisser Lösungen eine hervorragende Rolle, und wir nehmen so gewahr, daß alte schwierige Probleme..., wenn auch in anderem als dem ursprünglich gemeinten Sinne, dennoch eine völlig befriedigende und strenge Lösung gefunden haben.

Diese merkwürdige Tatsache neben anderen philosophischen Gründen ist es wohl, welche in uns eine Überzeugung entstehen lässt, die jeder Mathematiker gewiss teilt, die aber bis jetzt wenigstens niemand durch Beweise gestützt hat — ich meine die Überzeugung, daß ein jedes bestimmte mathematische Problem einer strengen Erledigung notwendig fähig sein müsse, sei es, daß es gelingt, die Beantwortung der gestellten Frage zu geben, sei es, daß die Unmöglichkeit seiner Lösung und damit die Notwendigkeit des Misslingens aller Versuche dargetan wird. ...

Diese Überzeugung von der Lösbarkeit eines jeden mathematischen Problems ist uns ein kräftiger Ansporn während der Arbeit; wir hören in uns den steten Zuruf: Das ist das Problem, suche die Lösung. Du kannst sie durch reines Denken finden; denn in der Mathematik gibt es kein Ignorabismus!“

---

[1]) Nach einem Vortrag, gehalten am 18.10.70 in Basel anlässlich der 150. Jahresversammlung der Schweizerischen Naturforschenden Gesellschaft.

[2]) Siehe Literaturverzeichnis!

Später heißt es:

„10. Entscheidung der Lösbarkeit einer diophantischen Gleichung. Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoeffizienten sei vorgelegt; man soll ein Verfahren angeben, nach welchem sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung im ganzen rationalen Zahlen lösbar ist."

Eine diophantische Gleichung ist von der Gestalt $f(x_1, ..., x_n) = 0$, wobei f ein Polynom mit ganzen (rationalen) Koeffizienten in den Variablen (Unbestimmten) $x_1, ..., x_n$ ist. Hilbert wünscht ein Verfahren, mit dessen Hilfe man entscheiden kann, ob $f = 0$ in *ganzen* Zahlen lösbar ist. Es ist nun z.B. $f(x, y) = 0$ in ganzen Zahlen genau dann lösbar, wenn wenigstens eine der Gleichungen $f(x, y) = 0, f(-x, y) = 0, f(x, -y) = 0, f(-x, -y) = 0$ in *natürlichen* Zahlen (0, 1, 2, ...) lösbar ist, und dies ist genau dann der Fall, wenn die Gleichung $f(x, y) \cdot f(-x, y) \cdot f(x, -y) \cdot f(-x, -y) = 0$ in natürlichen Zahlen lösbar ist. Ein Verfahren, um für beliebige diophantische Gleichungen die Lösbarkeit in natürlichen Zahlen zu entscheiden, liefert demnach auch ein Verfahren, um für beliebige diophantische Gleichungen die Lösbarkeit in ganzen Zahlen zu entscheiden. Es gilt auch die Umkehrung dieser Aussage: Es ist z.B. $f(x, y) = 0$ in natürlichen Zahlen genau dann lösbar, wenn $f(x_1^2+x_2^2+x_3^2+x_4^2, y_1^2+y_2^2+y_3^2+y_4^2) = 0$ in ganzen Zahlen lösbar ist [1]).

Nach dem Vorangehenden ist es gleichgültig, ob man nach einem Verfahren fragt, um die Lösbarkeit in ganzen oder in natürlichen Zahlen zu entscheiden. Wir wollen im Folgenden nach der *Lösbarkeit in natürlichen Zahlen* fragen. Unter einem *Hilbertschen Algorithmus* wollen wir ein Verfahren verstehen, mit dessen Hilfe man die Lösbarkeit einer diophantischen Gleichung in natürlichen Zahlen entscheiden kann.

Drei Beispiele für lösbare bzw. unlösbare diophantische Gleichungen:

(1) $x^2 - 17y^2 - 1 = 0$ ist lösbar. Eine Lösung ist $x = 1, y = 0$.

(2) $(x+1)^2 + (y+1)^2 - (z+1)^2 = 0$ ist lösbar. Eine Lösung ist $x = 2, y = 3, z = 4$.

(3) $(x+1)^3 + (y+1)^3 - (z+1)^3 = 0$ ist unlösbar.

---

[1]) Nach Lagrange ist jede natürliche Zahl als Summe von 4 Quadraten darstellbar.

Die Lösbarkeitseigenschaft einer diophantischen Gleichung ist ein 1-stelliges Prädikat L, welches z.B. auf die Gleichungen (1) und (2) zutrifft und auf (3) nicht zutrifft. Die Aussage *es gibt einen Hilbertschen Algorithmus* ist äquivalent zur Aussage *L ist ein entscheidbares Prädikat.*

2. *Übersicht.* Anfang diesen Jahres ist es dem russischen Mathematiker *Matijasevič* gelungen zu zeigen, daß L unentscheidbar ist (d.h., daß kein Hilbertscher Algorithmus existiert). Das wesentliche Hilfsmittel ist die 1936/7 ff von *Turing*, *Church* und vielen anderen geschaffene *Theorie der Entscheidbarkeit.* Später hat sich insbesondere *Julia Robinson* um das zehnte Hilbertsche Problem verdient gemacht. Eines ihrer Resultate besagt im Zusammenhang mit anderen Ergebnissen, daß kein Hilbertscher Algorithmus existiert, wenn ein Prädikat R mit bestimmten Eigenschaften existiert. Es ist dann Matijasevič gelungen, mit zahlentheoretischen Methoden ein solches Prädikat zu konstruieren.

3. *Ein Satz von Julia Robinson* (vorgetragen auf dem internationalen Mathematikerkongress in Cambridge/Mass, 1950; [5]). Wir betrachten Prädikate über natürlichen Zahlen, z.B. die 1-stelligen Prädikate *x ist eine Primzahl*, *Kx (x ist eine Kubikzahl)*, die 2-stelligen Prädikate $x = y$, $x \leqq y$, $x \mid y$ (teilt), und die 3-stelligen Prädikate $Sxyz$ (d.h. $x+y=z$), $Pxyz$ ($x \cdot y = z$), $Exyz$ ($x^y = z$), U_x ($x = 1$). Einige dieser Prädikate lassen sich durch Definitionen auf andere zurückführen. So gilt z.B. [1])

$$x \leqq y \leftrightarrow \bigvee z\, Sxzy\,, \tag{4a}$$

$$x \mid y \leftrightarrow \bigvee z\, Pxzy\,, \tag{4b}$$

$$Kx \leftrightarrow \bigvee y \bigvee z\,(Pyyz \wedge Pzyx)\,, \tag{5}$$

$$x \neq 0 \leftrightarrow \bigvee y \bigvee z\,(U_y \wedge S_{xyz})\,. \tag{6}$$

Nach *Tarski* heisst ein Prädikat R durch die Prädikate $R_1, \ldots, R_l$ *existentiell definierbar*, wenn es möglich ist R durch $R_1, \ldots, R_l$ so zu definieren, daß im Definiens höchstens die logischen Symbole $\bigvee$, $\wedge$, $\vee$ (also nicht $\bigwedge$, $\neg$) auftreten. Die Beziehungen (4), (5), (6) zeigen, daß $\leqq$ durch S sowie $\mid$ und K durch P existentiell definierbar sind,

Ein Prädikat A (über dem Bereich der natürlichen Zahlen) heißt *diophantisch*, wenn es durch S, P, U existentiell definierbar ist. A heißt *exponen-*

[1]) Wir verwenden die logischen Symbole $\neg$ (nicht), $\wedge$ (und), $\vee$ (oder), $\rightarrow$ (wenn-so), $\leftrightarrow$ (genau dann, wenn), $\bigwedge x$ (für alle x), $\bigvee x$ (es gibt ein x).

tiell diophantisch, wenn A durch S, P, E existentiell definierbar ist. $\leqq$, $|$, K und $\neq 0$ sind also diophantisch (und damit auch exponentiell diophantisch, da U exponentiell diophantisch ist).

Satz von J. Robinson: Wenn ein Hilbertscher Algorithmus existiert, so ist jedes diophantische Prädikat entscheidbar.

Beweis: Wir nehmen an, daß die Lösbarkeit jeder diophantischen Gleichung entscheidbar ist. A sei ein beliebiges n-stelliges diophantisches Prädikat. Es gibt also eine existentielle Definition von A durch S, P, U. Aus logischen Gründen kann man dabei annehmen, daß alle Existenzquantoren des Definiens am Anfang stehen („Normalform"). Damit sieht eine solche Definition von A so aus:

$$Ax_1 \dots x_n \leftrightarrow \vee y_1 \dots \vee y_l \alpha\,, \tag{7}$$

wobei der *Kern* α mit Hilfe von S, P, U den Variablen $x_1, \dots, x_n, y_1, \dots, y_l$ und den logischen Symbolen $\wedge$, $\vee$ gebildet ist. Die atomaren (d.h. von $\wedge$, $\vee$ freien) Bestandteile von α haben die Gestalt $u + v = w$, $u \cdot v = w$, bzw. $u = 1$ (wobei $u, v, w \in \{x_1, \dots, y_l\}$), also die Gestalt $p = 0$, wobei p ein Polynom ist. Diese speziellen Gleichungen werden in α mit Hilfe von aussagenlogischen Verknüpfungen $\wedge$, $\vee$ kombiniert. Nun ist offenbar (im Reellen)

$$p_1 = 0 \wedge p_2 = 0 \leftrightarrow p_1^2 + p_2^2 = 0\,,$$

$$p_1 = 0 \vee p_2 = 0 \leftrightarrow p_1 p_2 = 0\,.$$

Daher kann man annehmen, daß der Kern α die Gestalt $p = 0$ hat, wobei p ein Polynom in den Variablen $x_1, \dots, y_l$ ist. Damit haben wir die Darstellung

$$Ax_1 \dots x_n \leftrightarrow \vee y_1 \dots \vee y_l\, p(x_1, \dots, x_n, y_1, \dots, y_l) = 0\,. \tag{8}$$

Wir wollen zeigen, daß A entscheidbar ist, d.h. daß man für beliebige gegebene natürliche Zahlen $x_1, \dots, x_n$ mit einem endlichen Verfahren entscheiden kann, ob $Ax_1 \dots x_n$. Nun ist nach (8) die Behauptung $Ax_1 \dots x_n$ äquivalent zu der Aussage, daß die diophantische Gleichung $p(x_1, \dots, x_n, y_1, \dots, y_l) = 0$ mit gegebenen $x_1, \dots, x_n$ und den Variablen $y_1, \dots, y_l$ lösbar ist, was nach Voraussetzung entscheidbar ist.

3. *Aufzählbare Prädikate.* Wir werden im folgenden den Begriff des *aufzählbaren Prädikats* einführen. Man kann zeigen:

(9) Es gibt ein nicht entscheidbares aufzählbares Prädikat über den natürlichen Zahlen.

(10) Jedes aufzählbare Prädikat über den natürlichen Zahlen ist diophantisch.

Aus (9) und (10) folgt, daß es ein nicht entscheidbares diophantisches Prädikat gibt, woraus sich mit dem Satz von J. Robinson die Nichtexistenz eines Hilbertschen Algorithmus ergibt.

Wir wollen uns zunächst mit dem Begriff des aufzählbaren Prädikats beschäftigen und die bereits seit dem Beginn der Entscheidbarkeitstheorie bekannten Aussage (9) nachweisen. Zu (10) vgl. Nr. 4 und Nr. 5.

Ein n-stelliges Prädikat A heißt *aufzählbar*, wenn es eine systematische Erzeugung aller n-Tupel gibt, auf welche A zutrifft.

Beispiel 1. Das in Nr. 1 eingeführte einstellige Prädikat L ist aufzählbar. Man kann nämlich zunächst alle diophantischen Gleichungen (mit einem lexikographischen Verfahren) in eine Reihenfolge $D_0, D_1, D_2, \ldots$ bringen. Dann prüfe man für jedes k, beginnend mit $k = 0, 1, 2, \ldots$, ob es eine Lösung von D_0 oder ... oder von D_k gibt, bei der alle Variablen nur Werte $0, \ldots, k$ annehmen. Für jedes k ist diese Prüfung in endlich vielen Schritten durchführbar. So kann man die diophantischen Gleichungen, auf welche L zutrifft, systematisch erzeugen.

Beispiel 2. Jedes diophantische Prädikat A ist aufzählbar (Umkehrung von (10)). Um dies einzusehen, gehe man aus von einer Darstellung (8). Man suche für jedes k, beginnend mit $k = 0, 1, 2, \ldots$, im Bereich $0, \ldots, k$ Zahlen $x_1, \ldots, x_k, y_1, \ldots, y_l$ derart, daß $p(x_1, \ldots, y_l) = 0$. Für jedes k sind alle diese $x_1, \ldots, y_l$ in endlich vielen Schritten auffindbar. Jedes solche $(n+l)$-Tupel $x_1, \ldots, y_l$ liefert ein n-Tupel $x_1, \ldots, x_n$, auf welches A zutrifft. Mit dem angegebenen Verfahren lassen sich alle n-Tupel, auf welche A zutrifft, systematisch erzeugen.

Um (9) nachzuweisen, benötigen wir den Begriff der *Turingsmaschine* M (*Turing*, 1936; Einführungen in [1] oder [2]). M ist ein idealisierter Computer, der rein mathematisch wie folgt beschrieben werden kann [1]): M ist eine

[1]) Zur Veranschaulichung der nachstehenden Begriffe kann man sich vorstellen, daß M auf einem Rechenband operiert, das linear in Felder aufgeteilt ist, die durch ganze Zahlen charakterisiert sind. Eine Konfiguration $K = <\varphi, p, q>$ bestimmt (1) eine *Inschrift*, bei der auf dem $\bar{p}$-ten Feld das *Symbol* φ $(\bar{p})$ steht, (2) ein *Arbeitsfeld* p, (3) einen *Zustand* q. Bei der durch K bestimmten Zeile $q\ \varphi\ (p)\ v\ q'$ von M ist v das vorgeschriebene

beliebige Matrix mit 4 Spalten und $2(s+1)$ Zeilen, wobei es zu jedem Paar $\langle q, a \rangle$ mit $q \in \{0, ..., s\}$ und $a \in \{0, 1\}$ genau eine Zeile $qavq'$ in M gibt, wobei $v \in \{0, ..., 4\}$ und $q' \in \{0, ..., s\}$.

Wir verwenden im folgenden

q als Variable für die Elemente der Menge $\{0, ..., s\}$,

a als Variable für die Elemente der Menge $\{0, 1\}$,

v als Variable für die Elemente der Menge $\{0, 1, 2, 3, 4\}$,

p als Variable für die Elemente der Menge I der ganzen Zahlen,

φ als Variable für die Elemente der Menge der Abbildungen von I in $\{0, 1\}$.

Jedes Tripel $K = \langle \varphi, p, q \rangle$ heiße eine *Konfiguration von M*. K bestimmt eindeutig die mit $q, \varphi(p)$ beginnende Zeile von M, welche $q\,\varphi(p)\,v\,q'$ laute. Wenn $v = 4$, so heisse K eine *Endkonfiguration*. Eine Endkonfiguration hat keine *Folgekonfiguration*. Jede Konfiguration K, welche keine Endkonfiguration ist, hat eine eindeutig bestimmte Folgekonfiguration $F(K) = \langle \varphi^*, p^*, q^* \rangle$, mit $q^* = q'$ und

$$\begin{array}{llll} \text{falls } v = 0, & \text{so } p^* = p & \text{und} & \varphi^* = {}_0\varphi, \\ \text{„ } v = 1, & \text{„ } p^* = p & \text{„} & \varphi^* = {}_1\varphi, \\ \text{„ } v = 2, & \text{„ } p^* = p - 1 & \text{„} & \varphi^* = \varphi, \\ \text{„ } v = 3, & \text{„ } p^* = p + 1 & \text{„} & \varphi^* = \varphi, \end{array}$$

wobei ${}_0\varphi(p) = 0$ und ${}_1\varphi(p) = 1$ und ${}_0\varphi$ und ${}_1\varphi$ für die anderen Argumente dieselben Werte hat, wie φ.

Wir gehen nun aus von einer beliebigen natürlichen Zahl k. Diese Zahl k bestimmt eine Konfiguration $K_0 = \langle \varphi_0, p_0, q_0 \rangle$, wobei $q_0 = p_0 = 0$ und

$$\varphi_0(p) = \begin{cases} 1 & \text{für } 1 \leq p \leq k \\ 0 & \text{sonst.} \end{cases}$$

Es gibt dann eine Folge von Konfigurationen $K_0, K_1 = F(K_0), K_2 = F(K_1)$, ..., die evtl. mit einer Endkonfiguration $K_m = F(K_{m-1})$ abbricht $(m \geq 0)$.

Verhalten im nächsten Rechenschritt. $v = 4$ bedeutet *Stop*. $v = 0$ bzw. 1 bedeutet, daß auf dem Arbeitsfeld (welches als solches bleibt) das bisherige Symbol gelöscht und das neue Symbol 0 bzw. 1 gedruckt werden soll. $v = 2$ bzw. 3 bedeutet, daß die Inschriften nicht geändert, aber als neues Arbeitsfeld das mit der vorangehenden bzw. nachfolgenden Nummer gewählt werden soll. Schliesslich geht M in den neuen Zustand q' über.

Wenn K_j existiert, so sagen wir, daß M, *angesetzt auf* k, *wenigstens* j *Schritte durchführt*. Wenn die obige Folge mit einer Endkonfiguration abbricht, und dabei $\varphi_m(p_m) = a$, so sagen wir, daß M, *angesetzt auf* k, *das Resultat* a *liefert*.

Ein (hier der Einfachheit halber als 1-stellig vorausgesetztes) Prädikat A über den natürlichen Zahlen heißt *Turing-entscheidbar*, wenn es eine Turingmaschine M gibt derart, daß für jedes k gilt: Setzt man M auf k an, so liefert M das Resultat 0 bzw. 1 je nachdem, ob A auf k zutrifft oder nicht.

Wir definieren nun ein 1-stelliges Prädikat A_0 über den natürlichen Zahlen, welches aufzählbar, aber nicht entscheidbar ist. Man kann die Turingmaschinen (indem man diese Matrizen in geeigneter Weise „linearisiert") effektiv in einer Reihenfolge $M_0, M_1, M_2, \ldots$ anordnen. Nun sei R_0 dadurch definiert, daß für jede natürliche Zahl x gefordert wird:

(11) $A_0x \leftrightarrow$ die Turingmaschine M_x liefert, angesetzt auf x, das Resultat 1.

A_0 ist aufzählbar: Für jedes k, beginnend mit $k = 0, 1, 2, \ldots$, lasse man $M_0, \ldots, M_k$, angesetzt auf 0 bzw. ... bzw. k, k Schritte laufen (falls die Maschine nicht schon früher eine Endkonfiguration erreicht). Man notiere dabei die Zahlen j, bei denen M_j nach höchstens k Schritten mit dem Resultat 1 stehen bleibt. Damit hat man eine systematische Erzeugung der x_j, auf die A_0 zutrifft.

A_0 ist nicht Turing-entscheidbar: Sonst gäbe es eine Maschine M, welche, angesetzt auf eine beliebige Zahl k, das Resultat 0 bzw. 1 liefert, je nachdem ob A_0 auf k zutrifft oder nicht. Es gibt eine Zahl x mit $M = M_x$. Damit liefert M_x, angesetzt auf x, das Resultat 0 genau dann, wenn A_0x, d.h. (nach der Definition von A_0) von M_x, angesetzt auf x, das Resultat 1 liefert. Widerspruch.

A_0 ist nicht entscheidbar: Nach der *Churchschen These* (1936), welche eine Erfahrungstatsache ausdrückt, ist jedes entscheidbare Prädikat auch Turing-entscheidbar. Wir haben aber soeben gezeigt, daß A_0 nicht Turing-entscheidbar.

4. *Verschiedene Charakterisierungen der aufzählbaren Prädikate über den natürlichen Zahlen* (Literaturangaben hierzu in der zusammenfassenden Darstellung [6]). Es ist das Ziel, die Behauptung (10) nachzuweisen. Da die Umkehrung von (10) gilt (vgl. Beispiel 2 von Nr. 3), handelt es sich letztlich darum, die aufzählbaren Prädikate zu charakterisieren durch die Eigenschaft, diophantisch zu sein. Wir wollen zunächst einige andere Charakterisierungen der aufzählbaren Prädikate erwähnen, die als wichtige Zwi-

schenstufen angesehen werden müssen. Bereits in den Anfängen der Theorie der Entscheidbarkeit fand man:

(12) A ist aufzählbar *gdw* [1]) es gibt ein 2-stelliges entscheidbares Prädikat B derart, daß für jedes x:
$Ax \Leftrightarrow \bigvee y Bxy$.

Eine Beziehung zu diophantischen Prädikaten stellte 1950 *Davis* her:

(13) A ist aufzählbar *gdw* es gibt ein 3-stelliges diophantisches Prädikat D derart, daß für jedes x:
$Ax \Leftrightarrow \bigvee y \bigwedge z\,(z \leq y \rightarrow Dxyz)$.

Mit Hilfe von (13) bewiesen 1960 *Davis*, *Putnam* und *J. Robinson*:

(14) A ist aufzählbar *gdw* A ist exponentiell diophantisch.

(Zu dem Begriff „exponentiell diophantisch" vgl. Nr. 2. Die Implikation von rechts nach links in (14) lässt sich analog zu den Ausführungen in Beispiel 2, Nr. 3 trivial nachweisen). (14) zeigt, daß man jedes aufzählbare Prädikat durch S, P, E existentiell definieren kann. Um das gewünschte Endergebnis zu erhalten, genugt es nun zu zeigen, daß E existentiell durch S, P, U definierbar ist, d.h. diophantisch ist. Hierzu hatte Julia Robinson bereits im Jahre 1951 bewiesen:

(15) Das Prädikat E ist diophantisch, wenn es ein 2-stelliges diophantisches Prädikat R gibt, welches den beiden folgenden Bedingungen genügt:

(I) $\bigvee n \bigwedge x \bigwedge y\,(Rxy \rightarrow y \leq x * n)$,

(II) $\neg \bigvee n \bigwedge x \bigwedge y\,(Rxy \rightarrow y \leq x^n)$.

In (I) tritt die „Superpotenz" $*$ auf. Diese Funktion wird rekursiv definiert durch

(16)
$$\begin{cases} x * 0 = 1 \\ x * (n+1) = x^{x*n}. \end{cases}$$

Die Bedingung (I) besagt, daß bei Rxy die Zahl y durch x abgeschätzt werden kann, daß m.a.W. R in der zweiten Stelle nicht zu stark wächst. (II) besagt, daß eine solche Abschätzung nicht durch eine triviale Potenz x^n erreicht werden kann, daß also R in der zweiten Stelle nicht zu schwach wächst.

---

[1]) Genau dann, wenn.

5. *Das Ergebnis von Matijasevič.* Matijasevič [4] ist es 1970 gelungen, ein Prädikat R anzugeben, welches den beiden oben genannten Bedingungen (I), (II) von J. Robinson genügt. Zur Definition von R greift er zurück auf die bekannte Zahlenfolge φ_n von *Fibonacci* (um 1200), welche rekursiv definiert wird durch

$$\varphi_0 = 0, \varphi_1 = 1, \varphi_{n+2} = \varphi_n + \varphi_{n+1} . \tag{17}$$

Mit Hilfe dieser Folge wird R eingeführt durch:

$$Rxy \leftrightarrow \varphi_{2x} = y . \tag{18}$$

Es ist leicht einzusehen, daß die Wachstumsbedingungen (I) (für $n=3$) und (II) von (15) gelten. Das Problem liegt darin, einzusehen, daß R diophantisch ist. Hierzu betrachtet Matijasevič die Folge von „Psibonacci" $\Psi_n = \varphi_{2n}$, welche offenbar den Bedingungen $\Psi_0 = 0$, $\Psi_1 = 1$, $\Psi_{n+2} = 3\,\Psi_{n+1} - \Psi_n$ genügt, verallgemeinert diese durch die Definition:

$$\Psi_{m,0} = 0, \Psi_{m,1} = 1, \Psi_{m,n+2} = m\Psi_{m,n+1} - \Psi_{m,n} , \tag{19}$$

und zeigt

$$\begin{aligned} Rxy \ gdw \ \bigvee g \bigvee h \bigvee l \bigvee m \bigvee u \bigvee v \,(&x \leqslant y \wedge y < l \wedge l^2 | g \\ &\wedge \bigvee s\, l = \varphi_{2s+1} \wedge \bigvee k\,(g = \varphi_{2k+1} \wedge h = \varphi_{2k}) \\ &\wedge 2h + g \,|\, m - 3 \wedge l \,|\, m - 2 \wedge m \geqq 3 \wedge \bigvee n\, u = \Psi_{mn} \\ &\wedge x = Rest\,(u)\ mod\ l \wedge y = Rest\,(v)\ mod\ 2h + g) . \end{aligned} \tag{20}$$

Nun folgt unmittelbar, daß R diophantisch ist, wenn man die folgenden Beziehungen hinzunimmt:

$$\bigvee s\, l = \varphi_{2s+1} \leftrightarrow \bigvee z\, l^2 = 1 + lz + z^2 \tag{21}$$

$$\bigvee k\,(g = \varphi_{2k+1} \wedge h = \varphi_{2k}) \leftrightarrow g^2 = 1 + gh + h^2 \tag{22}$$

$$m \geqq 3 \rightarrow \left(\bigvee n\, u = \Psi_{mn} \leftrightarrow \bigvee v\,(u^2 + v^2 = 1 + muv)\right) . \tag{23}$$

Matijasevič arbeitet im wesentlichen mit Teilbarkeitseigenschaften der Fibonaccischen Zahlen, um (20) ... (23) herzuleiten (man hat z.B. $\varphi_s \mid \varphi_t \leftrightarrow s \mid t$ für $s, t \geqq 3$).

Davis hat gezeigt, daß man an Stelle der Fibonaccischen Zahlen auch mit den Lösungen geeigneter Pellscher Gleichungen $x^2 = (a^2-1)\,y^2 + 1$ operieren kann, welche übrigens für die Beweise der in Nr. 4 genannten Resultate von deren Autoren herangezogen worden sind.

Der Nachweis für die Nichtexistenz eines Hilbertschen Algorithmus ist ein schönes Beispiel für das Zusammenwirken von Methoden der Theorie der Entscheidbarkeit und der elementaren Zahlentheorie.

LITERATUR

[1] DAVIS, M. Computability and Unsolvability, McGraw-Hill, New York (1958).
[2] HERMES, H. Aufzählbarkeit, Entscheidbarkeit, Berechenbarkeit, *Heidelberger Taschenbücher 87*, Springer, Heidelberg (1971).
[3] HILBERT, D. *Gesammelte Werke*, Bd. 3. Springer, Heidelberg (1970).
[4] MATIJASEVIČ, J. V. Enumerable sets are diophantic. *Soviet Math. Dokl. 11* (1970), 345-357.
[5] ROBINSON, J. Diophantine Decision Problems. In: *Studies in Math.*, Vol. 6: *Studies in Number Theory*, ed. LeVeque (1969), 76-116.
[6] —— Existential Definability in Arithmetic. *Trans. Amer. Math. Soc. 72* (1952), 437-449.

(Reçu le 16 octobre 1971)

Hans Hermes
Mathematisches Institut der Universität
D-78 Freiburg i. Br.